## IN THE SPECIFICATION

- **Please amend the specification at PAGE 18, LINE 12 to PAGE 19, LINE 2 as follows:**

Where strong identification of a user or other entity that an access filter 203 communicates with is required, VPN 201 employs the Simple Key Management for Internet Protocols (SKIP) software protocol, developed by Sun Microsystems, Inc. The protocol manages public key exchange, authentication of keys, and encryption of sessions. It does session encryption by means of a transport key generated from the public and private keys of the parties who are exchanging data. Public keys are included in X.509 certificates that are exchanged between SKIP parties using a separate protocol known as the Certificate Discovery Protocol (CDP). A message that is encrypted using SKIP includes in addition to the encrypted message an encrypted transport key for the message and identifiers for the certificates for the source and destination of the data. The recipient of the message uses the identifiers for the certificate of the source of the message to locate the public key for the source, and uses its keys and the source's public key to decrypt the transport key and uses the transport key to decrypt the message. A SKIP message is in the sense that it contains an authentication header which includes a cryptographic digest of the packet contents and modification of any kind will render the digest incorrect. SKIP is discussed in detail in "Simple Key-Management for Internet Protocols (SKIP)" by Ashar Aziz and Martin Patterson. ~~For details on SKIP, see Ashar Aziz and Martin Patterson, Simple Key-Management for Internet Protocols (SKIP), which could be found on 2/28/98 at http://www.Skip.Org/inet-95. html. For details on X. 509 certification, see the description that could be found on 9/2/97 at http://www. Rnbo.Com/PROD/rmadillo/p/pdoc2. htm.~~

- **Please amend the specification at PAGE 82, LINE 16-20 as follows:**

The forms of the policy request messages 2613 and the policy response messages 2615 are defined by a policy protocol. Examples of standard policy protocols that are presently being developed are COPS (Common Open Policy System)~~, which is available at http://www.ietf. Of June 21,1999)~~ and RADIUS (Remote Authentication Dial In User Service, Internet standard RFC2138).

- **Please amend the specification at PAGE 118, LINE 30-33 as follows:**

Giving a user who is a member of the Bind Neptune user group access to WS://Bind Neptune.html involves the following steps:

1. User enters URL for the resource in the user's Web browser ~~(http://pluto.interdyn.com/Bind Neptune.html)~~;

- **Please amend the specification at PAGE 99, LINE 1-9 as follows:**

FIG. 54 shows virtual relational database system 5401 with VDB service 3813 and virtual relational database table 5411. Virtual relational database table 5411 does not really exist, but appears to exist to the applications that make queries on it. From the application's point of view application, virtual relational database table 5411 works exactly like a real relational database table ~~5411~~. Virtual relational database table 5411 appears to include some number of virtual rows 5413 (0 . . . q) each of which has a number of fields 5415 (0 . . . p). When a user makes a query on virtual table 5411, the query's WHERE clause determines which of the rows 5413 is selected and the SELECT clause determines which fields 5415 of the selected rows are returned.